

REMARKS

[0001] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-5, 8-17 and 19-32 are presently pending. Claims amended herein are: 1, 14, 22 and 28. Claims withdrawn or cancelled herein are: None. New claims added herein are: None.

Formal Request for an Interview

[0002] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0003] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Claim Amendments

[0004] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 14, 22 and 28 herein.

Substantive Matters

Claim Rejections under §101

[0005] Claims 22-27 are rejected under 35 U.S.C. §101. In light of the amendments presented herein, Applicant respectfully submits that these claims comply with the patentability requirements of §101 and that the §101 rejections should be withdrawn. The Applicant further asserts that these claims are allowable. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0006] The Examiner indicated (Action, p. 3-4) the following with regard to this claim:

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 22 teaches a system comprised of a first security engine, a second security engine and an event manager. The specification defines security engines as "implemented in software, hardware, or a combination of both." It is further stated, that the event manager receives events from the security engines and then "processes these events and communicates the information contained in particular events to other search engines." The Examiner interprets the event manager to recite software. Therefore, the entire claim recites software, which fails to fall into one of the 4 categories of invention. The dependent claims 23-27 limit the software of independent claim 22, so they are non-statutory as well.

The rejection for claims 22-27 under 35 U.S.C. 101 stands as the amendment filed 2/23/2007 does not recite enough structure. The Examiner suggests modeling claim 22 after statutory claim 28.

To that end, independent claim 22 has been amended to model after claim 28 as suggested on p. 4 of the Action. If the Examiner maintains the rejection of these claims, then the Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under §§ 102 and/or 103

[0007] The Examiner rejects claims 14-17, 19-21 and 28-32 under §102. For the reasons set forth below, the Examiner has not shown that cited references anticipate the rejected claims.

[0008] In addition, the Examiner rejects claims 1-5, 8-13 and 22-27 under §103. For the reasons set forth below, the Examiner has not made a *prima facie* case showing that the rejected claims are obvious.

[0009] Accordingly, Applicant respectfully requests that the §102 and/or §103 rejections be withdrawn and the case be passed along to issuance.

[0010] The Examiner's rejections are based upon the following references alone and/or in combination:

- **Willebeek-LeMair:** *Willebeek-LeMair, et al.*, US Patent Publication No. 2003/0204632 (published October 30, 2003); and
- **Chen:** *Chen, et al.*, US Patent No. 4,970,504 (issued November 13, 1990).

Overview of the Application

[0011] The Application describes a technology for enhancing the security of a computing system by sharing events, such as security-related events, among multiple security engines. In a particular embodiment, an event is received from a first security engine. A second security engine is identified that can utilize

information contained in the event. The information contained in the event is then communicated to the second security engine.

Cited References

[0012] The Examiner cites Willebeek-LeMair as the primary reference in the anticipation- and/or obviousness-based rejections. The Examiner cites Chen as a secondary reference in the obviousness-based rejections.

Willebeek-LeMair

[0013] Willebeek-LeMair teaches a technology for network discovery functionality, intrusion detector functionality and firewalling functionality integrated together to form a network security system presenting a self-deploying and self-hardening defense for a network.

Chen

[0014] Chen teaches a technology for a security system for controlling access to property having a user-operated keyboard to key in and reset a composite password code. An indicator visually displays at least one code symbol varying with time. A memory device stores a current composite password code including at least two code symbols so that upon entry of the keyed-in password code through the keyboard, one of the stored password code symbols is replaced directly by the time varying code symbol to form a regenerated, composite

password code which is then compared with the keyed-in password code to grant access to the property when coincidence occurs between the keyed-in and the regenerated password codes. In response to non-coincidence, an alerting signal is generated to indicate the incorrect password condition.

Anticipation Rejections

[0015] Applicant submits that the anticipation rejections are not valid because, for each rejected claim, no single reference discloses each and every element of that rejected claim.¹ Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.²

Based upon Willebeek-LeMair

[0016] The Examiner rejects claims 14-17, 19-21 and 28-32 under 35 U.S.C. § 102(e) as being anticipated by Willebeek-LeMair. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejection of these claims.

Independent Claim 14

[0017] The Examiner indicates (Action, p. 4-5) the following with regard to this claim:

¹ "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); also see MPEP §2131.

² See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Claims 14-17, 19-21, and 28-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Willebeek-LeMair et al. (US 2003/0204632 A1) hereinafter Willebeek-LeMair.

Claim 14:

Paragraph [0014] teaches an intrusion detector functionality that sends an alert when detecting potentially harmful traffic. This is sent to a firewall, which responds by blocking the entrance of the detected traffic. The Examiner interprets the intrusion detector and firewall to be "security engines" of claim 1. This would then teach one security engine (intrusion detector) detecting an event (potentially harmful traffic), identifying a second security engine (firewall), and communicating the event to it. Paragraph [0075] teaches that the network discovery functionality maintains a database that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

[0018] Claim 14, as amended, recites a method including, *inter alia*, receiving a security-related event from a first security-related application program, the security-related event being associated with a system state; identifying information contained in the security-related event; identifying a second security-related application program associated with the information contained in the security-related event, wherein the second security-related application program is unaware of the first security-related application program; and communicating the information contained in the security-related event to the second security-related application program.

[0019] Willebeek-LeMair does not disclose a second security-related application program being unaware of a first security-related application program. Rather Willebeek-LeMair discloses an intrusion detector functionality 116 [i.e. the first security-related application program] and a firewalling functionality 118 [i.e. the second security-related application program] being interlocked such that the firewalling functionality 118 [i.e. the second security-related application program] can take alerts generated by the intrusion detector functionality 116 [i.e. the first security-related application program]. See ¶ [0052].

[0020] Consequently, Willebeek-LeMair does not disclose all of the claimed elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Independent Claim 28

[0021] Applicants respectfully contend that the arguments set forth above with respect to independent claim 14, as amended, applies with equal weight here and Willebeek-LeMair does not disclose all of the claimed elements and features of independent claim 28, as amended. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims

[0022] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0023] Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a *prima facie* case have not been met.

Based upon Willebeek-LeMair

[0024] The Examiner rejects claims 1-5, 8-13 and 22-27 under 35 U.S.C. § 103(a) as being unpatentable over Willebeek-LeMair in view of Chen. Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0025] The Examiner indicates (Action, p. 8-9) the following with regard to this claim:

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 8-13, and 22-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willebeek-Lemair as applied to claims 14-17, 19-21, and 28-32 above, and further in view of Chen (US 4, 970, 504) hereinafter Chen.

Claims 1 and 2:

Willebeek-LeMair paragraph [0014] teaches an intrusion detector functionality that sends an alert when detecting potentially harmful traffic. This is sent to a firewall, which responds by blocking the entrance of the detected traffic. The Examiner interprets the intrusion detector and firewall to be "security engines" of claim 1. This would then teach one security engine (intrusion detector) detecting an event (potentially harmful traffic), identifying a second security engine (firewall), and communicating the event to it.

Willebeek-LeMair does not teach but Chen teaches "the event corresponds to identifying a password that does not comply with a predetermined criteria" in Chen column 4 lines 11-31. The motivation to combine the two systems would be Chen column 4 lines 11-31 wherein the password being incorrect is an alarm condition in a security system and ways to determine the password being incorrect is when the "keyed-in password does not equal the currently stored password, including unequal number and inconsistent length".

[0026] Claim 1, as amended, recites a method including, *inter alia*, receiving an event from a first security engine; identifying a second security engine configured to utilize information contained in the event, wherein the

second security engine is unaware of the first security engine; and communicating the information contained in the event to the second security engine, wherein the event corresponds to identifying a password that does not comply with predetermined criteria.

[0027] As mentioned above, Willebeek-LeMair discloses an intrusion detector functionality 116 [i.e. the first security engine] and a firewalling functionality 118 [i.e. the second security engine] being interlocked such that the firewalling functionality 118 [i.e. the second security engine] can take alerts generated by the intrusion detector functionality 116 [i.e. the first security engine]. See ¶ [0052]. Further, were Willebeek-LeMair modified to include claim 1, i.e. were Willebeek-LeMair modified to include intrusion detector functionality 116 being unaware of firewalling functionality 118, Willebeek-LeMair would not achieve his desired result of firewalling functionality 118 dropping packets or shutting down the session or origin of the attack upon intrusion detector functionality 116 detecting imminent attack. See ¶ [0052].

[0028] As shown above, the combination of Willebeek-LeMair and Chen does not teach or suggest all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Independent Claim 22

[0029] Applicants respectfully contend that the arguments set forth above with respect to independent claim 1, as amended, applies with equal weight here and a *prima facie* case of obviousness is not present with respect to independent

claim 22, as amended. Accordingly, Applicant asks the Examiner to withdraw the rejection of the claims.

Dependent Claims

[0030] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0031] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action.** Please call/email me or my assistant at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Attorneys for Applicant

/Michael D. Carter/ _____ Dated: 7/3/08
Michael D. Carter (michaelcarter@leehayes.com; 512-505-8164)
Registration No. 56661
Emmanuel Rivera (emmanuel@leehayes.com; 512-505-8162)
Registration No. 45760

Customer No. **22801**

Facsimile: (509) 323-8979
www.leehayes.com